

# What is Future of SOC?

- It is an **intelligent, automated, and predictive** Cyber Security center.
- It integrates data from multiple sources (networks, cloud, endpoints, users).
- It transforms security from **reactive to proactive**, with AI-based decisions.

**Its main purpose:** to reduce detection times, response times, and workload.

## Main challenges for SOC

Hybrid infrastructures that are difficult to protect

High volume of alerts (+333M events / 6 months)

Lack of visibility and interoperability between tools

Regulatory pressure (GDPR, NIS2, CRA, etc)

" More than 90% of SOC's still rely on manual processes"

## Cyber threat transformation



Intensive use of AI by attackers.



Increase in exploited vulnerabilities  
(+55% in 2 years).



Explosion of attacks with stolen  
credentials (has multiplied by 5 in  
2 years).



Less time to act; from 9 days to less  
than 2.

71%

attacks with stolen  
credentials.

45%

of exfiltrations happen  
in <1 day.

## AI integrated Cyber Security evolution

- Artificial Intelligence and Machine Learning prioritize threats, reduce alerts, and improve response.
- False positives have been reduced.
- Use of LLMs to automate repetitive tasks.

20–40% of analyst tasks can be automated

Detection in 10 seconds | Response in 1 minute

## From Traditional SOC to the SOC of the Future

	Traditional SOC	SOC with AI
Processes	Manual	Automated
Visibility	Partial / in silos	Total and unified
Alerts	Excessive volume	Smart filtering
Reaction Time	Slow	Real time
Analysts	Overwhelmed	Supported by AI

## Modern SOC architecture

